IN THE SPECIFICATION

Please amend the specification as shown below.

Please replace the paragraph beginning on page 1, line 12 with the following:

The cyphering/decyphering algorithms to which the present invention applies are generally executed by integrated ~~circuit~~ circuits, either by means of state machines in wired logic, or by means of microprocessors executing a program in memory (generally a ROM). Such algorithms use secret keys specific to integrated circuits or to the user, which are exploited by the algorithm to code the data.

Please replace the paragraph beginning on page 2, line 30 with the following:

Examples of non-linear substitution transformations such as that disclosed hereabove are described, for example, in work "The Design of Rijndael" by Joan Daemen and Vincent Rijmen, published by Springer-Verlag (ISBN 3-540-42580-2) and in the AES standard (FIPS PUB 197), which references are incorporated herein by reference.

Please replace the paragraphs beginning on page 3, line 21 with the following:

A known weakness of implementations on smart cards of AES-type algorithms or more generally of algorithms implementing several turns or cycles of a same transformation (T) on a code divided into blocks, is the sensitivity to attacks by analysis of the current consumption of the circuit executing the algorithm. Such an attack known as a DPA (Differential Power Analysis) consists of correlating the power consumption of the integrated circuit executing the algorithm with the secret keys used upon cyphering or decyphering. In practice, based on a message to be cyphered and on hypotheses about the secret key, a statistic correlation curve is established along time between the power consumption of the product for the message cyphering

and an intermediary value calculated by the circuit. Such power consumption attacks are described in literature (see, for example, article "Differential Power Analysis" by Paul Kocher, Joshua Jaffe, and Benjamin Jun, published in 1999, CRYPTO Conference 99, pages 388-397, published by Springer-Verlag LNCS 1666), which is incorporated herein by reference.

Please replace the paragraphs beginning on page 6, line 18 with the following:

The present invention also aims at providing a solution which ~~minimizes~~ reduces the number of times that a substitution box must be calculated and/or stored.

The present invention also aims at ~~minimizing~~ reducing the calculation time necessary to the execution of the algorithm after introduction of the random number.

To achieve these and other objects, the present invention provides a cyphering/decyphering method, by an integrated circuit, of a digital input code by means of several keys, ~~consisting of~~ comprising:

Please replace the paragraph beginning on page 6, line 26 with the following:

applying to said blocks several turns of a cyphering or decyphering ~~consisting of~~ comprising submitting each block to at least one same non-linear transformation and of subsequently combining each block with a different key at each turn,

Please replace the paragraph beginning on page 7, line 3 with the following:

According to an embodiment of the present invention, said non-linear transformation ~~consists of~~ comprises using a box of substitution of the input code blocks, calculated with a third random number of same length as said code and all the blocks of which have the same value. According to the present invention, said box respects the fact that the transformation of an input

code, previously combined by XOR with the first random number, corresponds to the result of the combination by XOR of this input code with said third random number.

Please replace the paragraph beginning on page 8, line 13 with the following:

For clarity, only those steps that are necessary to the understanding of the present invention have been shown in the drawings and will be described hereafter. In particular, the processings upstream and downstream of the cyphering algorithm have not been detailed and are no object of the present invention. Further, the operations of division of the secret quantity into several sub-keys to be taken into account by the algorithm, as well as the generation of the adapted random numbers have not been ~~detailed~~ described in detail and are within the abilities of those skilled in the art based on the indications which will be given hereafter.

Please replace the paragraph beginning on page 9, line 22 with the following:

First step 41 ~~consists of~~ comprises performing an XOR-type combination of state S_0 with a random value R having the same size as state S_0 (for example, 128 bits).

Please replace the paragraph beginning on page 9, line 27 with the following:

The second phase of the cyphering method ~~consisting of~~ comprising executing n-1 turns of a same transformation T is then entered. This transformation involves the steps of the conventional process (for example, AES) which are desired to be masked by at least one random value. In the example shown, these are row shifting step 33 (SHIFTROWS), step 34 (SUBBYTES) of byte substitution by means of a substitution box SBOX, column mixing step 35 (MIXCOLUMNS), and step 36 of XOR combination (ADDROUNDKEY) with sub-key Ki of rank i.

Please replace the paragraph beginning on page 11, line 3 with the following:

There again, the present invention ~~consists of~~ comprises interposing, between some steps of the algorithm, the execution of which is desired to be masked by random values, logic combinations of the matrixes processed by values R1 and R2.

Please replace the paragraph beginning on page 12, line 26 with the following:

Of course, the present invention is likely to have various alterations, modifications, and ~~improvement~~ improvements which will readily occur to those skilled in the art. In particular, the present invention which has been described hereabove in relation with the AES-type cyphering algorithm may be transposed to any cyphering algorithm, the input code of which is divided into blocks of identical sizes to be ciphered, each block being submitted to a same non-linear transformation.

Please replace the paragraph beginning on page 13, line 6 with the following:

Finally, the present invention applies whatever the use made of the ~~ciphered~~ cyphered data.